(Rev. 01-31-2003)

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/26/2004

To: San Francisco

From: San Francisco
Squad 14G-Cybersquad, San Jose Resident Agency
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] wl

196551-01

Case ID #: 288A-SF-~~NEW~~ (Pending)

Title: UNSUB(S),
AKA MYDOOM VIRUS;
GOOGLE - VICTIM;
YAHOO - VICTIM;
LYCOS - VICTIM;
COMPUTER INTRUSIONS-CRIMINAL MATTERS

Synopsis: Request to open a new 288A case at San Francisco based on reports that users of popular internet search engines were unable to access major search engine websites or experienced slowness due to the MyDoom virus, which flooded major search engines with automated searches.

Enclosure(s): CNN.com website article (http://www.cnn.com) on the release and impact of the MyDoom virus, dated 07/26/2004.

Details: On 07/26/2004, CNN.com (http://www.cnn.com) reported that internet search engines, such as Google (http://www.google.com), Yahoo (http://www.yahoo.com), and Lycos (http://www.lycos.com) were unable to provide search results to a number of web surfers probably due to a new variant of the MyDoom virus. The problem began at approximately 11:30AM Eastern Time.

The virus uses search engines on infected computers to look for more e-mail addresses in order to keep replicating itself.

It is recommended that this matter be opened and assigned to SA [redacted]

♦♦

O+A as 288A-SF-NEW to SA [redacted]
MA 7/26/04

Opened & Assigned to SA [redacted]
07/26/04

5 - 208LMM2-EC
288A-SF-196551-01

- http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.m@mm.html
- http://www.f-secure.com/v-descs/mydoom_m.shtml

5. Attachments:

None.

TECHNOLOGY

TECHNOLOGY NEWS

Google: MyDoom virus caused problems

- Video coach prepares athletes for Athens
- Bloggers get convention credentials
- 'Bin Laden suicide' virus hits Web

TOP STORIES

CNN.com HOME PAGE

Dems stress unity in Boston

- **CNN/Money:** Big money behind conventions
- GOP: Kerry undergoing 'extreme makeover'
- Google blames MyDoom virus

International Edition | Languages | CNN TV | CNN International | Headline News | Transcripts | Preferences

SEARCH The Web CNN.com Search Powered by

b6
b7C

1A Envelope

Case ID: 288A-SF-136551-1A

SF	1	ORIGINAL NOTES RE INTERVIEW OF [redacted] LYCOS
SF	2	ORIGINAL NOTES RE INTERVIEW OF [redacted] GOOGLE LEGAL COUNSEL
SF	3	ORIGINAL NOTES RE INTERVIEW OF [redacted] MCAFEE
SF	4	STAS TECHNICAL LEAD ANALYSIS

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

FD-340a (Rev. 1-27-03)

(Title) _____

(File No.) 288A -SF- 136551

Item	Date Filed	To be returned Yes	To be returned No		Disposition

b6
b7C

1A4

FD-340 (Rev. 4-11-03)

File Number 288A-SF-136551

Field Office Acquiring Evidence SF

Serial # of Originating Document _____

Date Received 3/14/05

From Cyber - STAS, FBI HQ
(Name of Contributor/Interviewee)

(Address)

(City and State)

By SA [redacted]

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Title: MyDoom

Reference: _____
(Communication Enclosing Material)

Description: ☐ Original notes re interview of

STAS Technical Lead Analysis of MyDoom Virus

288A-SF-136551-1A4

FD-801 (Rev. 7-15-97)

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: Routine **Date:** 07/29/2004

To: Director, FBI **Attn:** Computer Investigations Unit, Room 11887
Computer Investigations and Infastructure
Threat Assessment Center
(CID/NSD)

MJM/ma

From: SAC, San Francisco

Approved By: [ ] MA

Drafted By: [ ]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

Case ID #: 288A-SF- 136551 - 03

Title: Subject: UNSUB(S), A.K.A. MyDoom Virus;
Victim: Google, Yahoo, Lycros, Altavista
Type: Computer Intrusion
Date: 07/26/2004

SUBMISSION: ☒ Initial ☐ Supplemental ☐ Closed

CASE OPENED: 07 / 26 / 2004

CASE CLOSED: ___ / ___ / ___

- ☐ No action due to state/local prosecution (Name/Number: _____)
- ☐ USA declination
- ☐ Referred to Another Federal Agency (Name/Number: _____)
- ☐ Placed in unaddressed work
- ☐ Closed administratively
- ☐ Conviction

COORDINATION: FBI Field Office: San Francisco
Government Agency:
Private Corporation:

VICTIM

Company name/Government agency: Google, Mt. View, CA; Yahoo, Santa Clara, CA;
Address/location: Altavista, Palo Alto, CA; Lycos, Waltham, MA

Purpose of System: Internet Search Engines
Highest classification of information stored in system: Unknown

To: Director, FBI From: SAC, San Francisco
Re: 288A-SF-136551 , Date 07/29/2004

System Data:

Hardware/configuration (CPU): Unknown
Operating System: _____
Software: _____

Security Features:

Security Software Installed: ☐ yes (identify Unknown) ☐ no
Logon Warning Banner: ☐ yes ☐ no

INTRUSION INFORMATION

Access for intrusion: ☒ Internet connection ☐ dial-up number ☐ LAN (insider)
If Internet: Internet address: _____
Network name: _____

Method:

Technique(s) used in intrusion: DDOS (list provided)

Path of intrusion:
addresses: 1. Distributed 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject: Unknown

Age: _____ Race: _____
Sex: _____ Education: _____
Alias(s): _____ Motive: _____
Group Affiliation: _____
Employer: _____
Known Accomplices: _____
Equipment used:
Hardware/configuration (CPU): _____
Operating System: _____
Software: _____

Impact:

Compromise of classified information: ☐ yes ☒ no
Estimated number of computers affected: Unknown
Estimated dollar loss to date: Unknown

To: Director, FBI From: SAC, San Francisco
Re: 288-A-SF-136559 Date 07/29/2004

Category of Crime:

Impairment:

- ☐ Malicious code inserted
- ☒ Denial of service
- ☐ Destruction of information/software
- ☐ Modification of information/software

Theft of Information:

- ☐ Classified information compromised
- ☐ Unclassified information compromised
- ☐ Passwords obtained
- ☐ Computer obtained
- ☐ Telephone services obtained
- ☐ Application software obtained
- ☐ Operating software obtained

Intrusion:

- ☐ Unauthorized access
- ☐ Exceeding authorized access

REMARKS

On 07/26/2004, popular internet search engines were unable to provide search results to a number of web surfers due to a new variant of the MyDoom virus.

The virus uses search engines to look for more e-mail addresses in order to keep replicating itself.

Menu
Technology(s) Used:

Top Screen Protocol Attacks:		*Secondary Screen*	
☒	IP	☐	spoofing attack
		☐	source routing
☒	TCP	☐	sequence number attack
☐	UDP	☐	spoofing attack
		☐	flooding
☐	FTP	☐	vulnerable version
		☐	SITE EXEC
		☐	overload FTP buffer
		☐	anonymous FTP
☐	Telnet	☐	highjacking
		☐	packet sniffing
☐	TFTP		
☐	r commands	☐	rsh
		☐	rlogin
☐	SMTP	☐	vulnerable version
		☐	spoofing
		☐	embedded postscript attack
		☐	trojan horse attack
		☐	syslog attack
		☐	flooding
		☐	MIME
☐	HTTP	☐	flooding
		☐	Telnet to HTTP port
☐	gopher		
☐	X11 window		

Top Screen

- ☐ DNS
- ☐ SNMP
- ☐ FSP
- ☐ NFS

Secondary Screen

- ☐ vulnerable version
- ☐ flooding

Other Attacks:

- ☒ Worm
- ☐ Social engineering
- ☐ Scavenging and reusing
- ☐ Masquerading
- ☐ Scanning
- ☐ Trojan Horse
- ☐ Other

288A-SF-136551

b6
b7C

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. 288A-SF-136551-4

450 Golden Gate Ave.
PO Box 36015
San Francisco, CA 94102
(415)553-7400
July 28, 2004

Attention: [redacted]
Lycos Legal Department

Dear [redacted]

This letter is to document the conversation yesterday, 07/27/2004, regarding our investigation into the impact of the MYDOOM COMPUTER VIRUS on your organization. Parties to the conversation included yourself, Special Agents [redacted] and [redacted].

If you have any further questions, or additional information, please contact Special Agent [redacted].

Sincerely,

Mark J. Mershon
Special Agent in Charge

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

By: [redacted]

[redacted]
Supervisory Special Agent

288A-SF-136551-4

HP OfficeJet K Series K80xi
Personal Printer/Fax/Copier/Scanner

Log for
HT Internet
[redacted]
Jul 28 2004 3:42pm

b6
b7C

Last Transaction

Date	Time	Type	Identification	Duration	Pages	Result
Jul 28	3:42pm	Fax Sent	[redacted]	0:22	1	OK

FD-302 (Rev. 10-6-95)

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/16/2004

On August 11, 2004, [redacted] Legal Counsel at Google, in Mountain View, California, telephone number 650/623-6048, was interviewed telephonically and advised of the identity of the interviewing agent and the nature of the interview. [redacted] provided the following information:

GOOGLE is not currently experiencing any affects from the MYDOOM virus that initially struck on July 26, 2004. [redacted] advised that representatives from GOOGLE are working on preparing an analysis of the financial loss suffered by GOOGLE due to the MYDOOM virus. [redacted] believes it will be approximately $100,000.

[redacted] advised that she has the IP addresses of the first ten hosts that queried the GOOGLE search engine related to the MYDOOM attack and said that she would send the information to me via email. The resulting email is attached to and made a part of this FD-302.

Investigation on 08/11/2004 at Quantico, Virginia (telephonically)

File # 288A-SF-136551 - 5 Date dictated 08/16/2004

by SA [redacted]

288A-SF-136551-5 [redacted] 231WL12.302.wpd

FD-302 (Rev. 10-6-95)

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/27/2004

On July 27, 2004, [redacted] LYCOS in San Francisco, California, telephone number (650)428-5000, was interviewed telephonically and advised of the identity of the interviewing agents and the nature of the interview. [redacted] provided the following information:

Between 8:30AM and 9:00AM Eastern Daylight Time (EDT) on 07/26/2004, the servers at Lycos were impacted by the MYDOOM virus. Between 9:00AM and 10:00AM eastern, legitimate web users' availability to search results conducted by LYCOS was at 37%. By 11:00AM eastern, availability was less than 4%.

By 7:30PM eastern, LYCOS had implemented filters on searches coming into the servers on certain text strings like "mail", "reply", "rcpt", and "contact" that they noted were being queried by the virus. By applying these filters, they were able to block the searches committed by the virus and allow regular users to access the search functions of LYCOS. LYCOS could not simply block an Internet Protocol (IP) address or range of IP addresses because of the distributed nature of the virus.

[redacted] noted that traffic to the LYCOS website was at approximately 50 times normal levels on 07/26/2004 and continues to fluctuate between 30 and 50 times normal levels on 07/27/2004, but that, due to the filters implemented by LYCOS, their search functions are running normally for most users.

Investigation on 07/27/2004 at San Jose, California (telephonically)

File # 288A-SF-136551 - 6 Date dictated 07/27/2004

by SA [redacted]:wl
SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted] 23/WL06.302.wpd 288A-SF-136551-6

FD-302 (Rev. 10-6-95)

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/27/2004

On July 27, 2004, [redacted] and [redacted] MCAFEE, telephone number (503)466-4484, were interviewed telephonically and advised of the identity of the interviewing agents and the nature of the interview. [redacted] and [redacted] provided the following information:

The 15th variant of the MYDOOM virus was first noticed by MCAFEE on July 26, 2004 at approximately 6:30AM pacific time. The virus affected major search engines while trying to search for additional email addresses to send itself to, as well as several corporate customers whose mail servers were temporarily overwhelmed.

The virus harvests email addresses from a local, infected computer, then searches the domain name of the email addresses through the major internet search engines, in an attempt to locate additional email addresses. While the search engines were flooded with searches, [redacted] and [redacted] believe they were not the primary target.

The virus also installs a backdoor on TCP Port 1034 that future users and/or viruses can exploit. MCAFEE has already seen viruses discovered on July 27, 2004 that exploit this open port, but does not think they were necessarily written by the same author as the MYDOOM virus.

[redacted] and [redacted] noted that there was nothing unique or identifying about the virus executable. They do not have the source code of the virus.

Investigation on 07/27/2004 at San Jose, California (telephonically)

File # 288A-SF-136551 - 17 Date dictated 07/27/2004

by SA [redacted] wlw2
SA [redacted] bts

b6
b7C

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE · Date: 12/17/2004

To: San Francisco

From: San Francisco
Squad 14G-Cybersquad, San Jose Resident Agency
Contact: SA [redacted]

Approved By: [redacted] mA

Drafted By: [redacted] wl 12

Case ID #: 288A-SF-136551-8 (Pending)

Title: UNSUB(S)
aka MYDOOM VIRUS;
GOOGLE - VICTIM;
YAHOO - VICTIM;
LYCOS - VICTIM;
COMPUTER INTRUSIONS-CRIMINAL MATTERS

Synopsis: Request to close captioned matter.

Details: At 11:30AM Eastern time on 07/26/2004, internet search engines Google (http://google.com), Yahoo (http://yahoo.com), and Lycos (http://lycos.com) were unable to provide search results to a number of users for several hours due to a variant of the MyDoom virus (Mydoom.m) and Zindos worm.

On 07/28/2004, Special Technologies and Applications Section (STAS) assistance was requested in analyzing the source code of Mydoom.m and Zindos.

On 12/14/2004, STAS advised that the analysis of Mydoom.m and Zindos was complete. Strings and source code of the virus/worm were examined for clues as to the identity of the author, but none were found.

Determination of the original author is therefore deemed impossible and the case is being closed.

♦♦

SF Field Intelligence Group

Potential Intel Value: Yes ☒ No ☒

Reviewed By: mA Date: 12/17/04

S-Drive Location: _____

Close 4
mA 12/17/04

Case closed on 03/21/05

[redacted] 352wl01.ec

288A-SF-136551-8

b6
b7C

288A-SF-136551 - 09
WL:wl

1

The following investigation was conducted by Special Agent [redacted]

On December 14, 2004, Special Agent [redacted] received from STAS the Technical Lead Report on the Analysis of Mydoom-M/Zindos Worms. The report found no clues as to the identity of the author of either computer worm. The report is attached to and made a part of this document.

[redacted] 350 w/ 03 ins 288A-SF-136551-09

b6
b7C

FEDERAL BUREAU OF INVESTIGATION
CYBERDIVISION
SPECIAL TECHNOLOGIES AND APPLICATIONS SECTION
TECHNICAL ANALYSIS UNIT
TECHNICAL LEAD REPORT

FOR LEAD PURPOSES ONLY

TO: [redacted] DISTRIBUTION TO: XXX	Date: 11/22/04
Submitter's Case Number: 288A-SF-136551	
RE: ANALYSIS OF MYDOOM-M/ZINDOS WORMS	
Title: Anaysis of Mydoom-m/zindos worms Electronic Location: \\smb00\cases\ProductReports\2004_Reports\STAS-	
PREPARED BY: [redacted]	PHONE NUMBER: [redacted]
APPROVED: XXX	PHONE NUMBER: XXX
STAS CONTROL FILE: 288A-SF-136551	PRIMARY REPORT ID: STAS04-XXX MATS ID: 2004-XXX

1. **Media Type and Quantity:** 1 CD w/zip file containing Mydoom-m worm

2. **Analysis Requested:**

   - Assist in analysis of Mydoom-M Virus
   - Obtain a copy of zindos worm and analyze

3. **Executive Summary:**

A copy of the Zindos worm was obtained. Both Zindos and Mydoom-m (provided) were analyzed using IDA Pro (static disassembly of binary). Strings and code were examined for clues as to the identity of the author, but none were found.

4. **Details of Analysis:**

Zindos worm

- A copy of the zindos worm was obtained from a 3ed party source.
- It was loaded into IDA Pro for disassembly and analysis
- Disassembly revealed that zindos goes into a tight loop (every 50ms) trying to connect to www.microsoft.com
- The code was examined looking for identifying information such as names, email addresses, comments or IP addresses that might help identify the author. None were found.

Mydoom-m worm

- The worm was run in isolation and network traffic was recorded. Without being able to reach the Internet, the worm performs lookups for the mail server (MX) for the following domains:

  13 cvs.tartarus.org: type MX, class inet
  13 gto.net.om: type MX, class inet
  13 kohls.com: type MX, class inet
  14 lebanon-online.com.lb: type MX, class inet
  14 msdirectservices.com: type MX, class inet
  17 petri.co.il: type MX, class inet
  14 target.com: type MX, class inet
  14 tucows.com: type MX, class inet
  13 ultraschallpiloten.com: type MX, class inet

  (the number in front is a count of the occurrences during the test run).

  [**Analyst Comment on above list:** It is likely that this is a list of known "open relays" at the time the worm was released. The intent is likely to use them to send the initial round of messages.]

- Mydoom-m was loaded into IDA Pro for disassembly and static analysis. A cursory analysis of the code was consistent with analysis provided by commercial anti-virus vendors and security organizations at

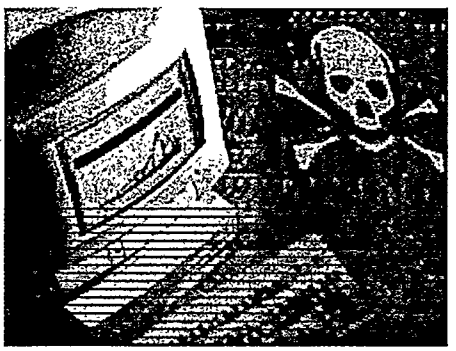
  - http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYDOOM.M

TECHNOLOGY

Google says MyDoom virus caused problems

Monday, July 26, 2004 Posted: 4:21 PM EDT (2021 GMT)

(CNN) -- The No. 1 Internet search engine on Monday was unable to provide search results to a number of Web surfers, probably because of a variant of the MyDoom virus.



Users of other popular search engines such as Yahoo and Lycos may also have experienced some sluggish behavior.

Google released a statement to CNN at 3 p.m. ET saying the site "experienced slowness for a short period of time early today because of the MyDoom virus, which flooded major search engines with automated searches.

"A small percentage of our users and networks that have the MyDoom virus have been affected for a longer period of time. At no point was the Google Web site significantly impaired, and service for all users and networks is expected to be restored shortly."

According to several media accounts, the problem began about 11:30 a.m. ET, and by 3 p.m. the site seemed to be running smoothly again.

The SANS Institute and other security firms issued a release shortly after the problem was detected saying a new variant of the MyDoom virus could be to blame. The latest incarnation of the troublesome virus uses search engines on infected computers to look for more e-mail addresses in order to keep replicating itself.

Experts contacted by CNN were unable to determine the exact magnitude of the problem.

Some users across the United States reported no trouble with Google or other search engines.

RELATED

• CNN/Money: Google IPO worth up to $3.3B

For other people, although the main Google page was able to load, they reported seeing a "server error" message when trying to conduct a search.

Google also announced details of its initial public offering Monday, with share prices of between $108 and $135. Experts consider those figures to be very high, leading some observers to initially speculate that Google was the victim of a vindictive hacker attack.

Story Tools
SAVE THIS E-MAILTHIS
PRINT THIS MOST POPULAR